

MODULES WITH MANY NON-ASSOCIATES AND NORM FORM EQUATIONS WITH MANY FAMILIES OF SOLUTIONS

PAUL M VOUTIER

To Wolfgang M. Schmidt, with warmest wishes and deepest admiration on his 80th birthday

ABSTRACT. For every number field \mathbb{K} , with $[\mathbb{K} : \mathbb{Q}] \geq 3$, we show that the number of non-associates of the same norm in a full module in \mathbb{K} does not depend only on \mathbb{K} , but can also depend on the module itself.

As a corollary, the same can be true for the number of families of solutions of degenerate norm form equations. So the uniform bound obtained by Schmidt for the number of solutions in the non-degenerate case does not hold always here.

For three-variable norm forms not arising from full modules, we do obtain a Schmidt-type bound for the number of families of solutions that, together with the above result, completes this aspect of the study of three-variable norm forms.

1. INTRODUCTION

1.1. Non-associates. Let \mathbb{K} be an algebraic number field with $r = [\mathbb{K} : \mathbb{Q}]$. Let $\alpha_1, \dots, \alpha_n$ lie in \mathbb{K} and put $L(\mathbf{X}) = \alpha_1 X_1 + \dots + \alpha_n X_n$.

The set $\mathcal{M} = \{L(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}^n\}$ is a \mathbb{Z} -module contained in \mathbb{K} .

For every subfield \mathbb{L} of \mathbb{K} , let $\mathcal{M}^{\mathbb{L}}$ consist of the elements β of \mathcal{M} such that for every $\alpha \in \mathbb{L}$ there is a non-zero rational integer z with $z\alpha\beta \in \mathcal{M}$.

Definition 1. We can associate with each $\mathcal{M}^{\mathbb{L}}$ a *ring of coefficients*, which we will denote by $\mathcal{O}_{\mathcal{M}}^{\mathbb{L}}$, i.e., the set of $\alpha \in \mathbb{L}$ such that $\alpha\beta \in \mathcal{M}^{\mathbb{L}}$ for every $\beta \in \mathcal{M}^{\mathbb{L}}$.

For our purposes here, we single out a particular subgroup of the group of units in \mathbb{L} : let $\mathcal{U}_{\mathcal{M}}^{\mathbb{L}}$ be the group of elements in $\mathcal{O}_{\mathcal{M}}^{\mathbb{L}}$ of norm 1.

Definition 2. We say that \mathcal{M} is a *full module* in \mathbb{K} if its rank, as a \mathbb{Z} -module, is equal to r .

Two elements μ_1 and μ_2 of a full module \mathcal{M} are called *associates* if there exists $\eta \in \mathcal{U}_{\mathcal{M}}^{\mathbb{K}}$ such that $\mu_1 = \eta\mu_2$.

Note that if \mathcal{M} is a full module, then $\mathcal{M}^{\mathbb{K}} = \mathcal{M}$.

It is known that there are only finitely many pairwise non-associate elements with given norm in a full module \mathcal{M} (see [1, Corollary to Theorem 5, pg. 90]).

While some upper bounds for the number of such non-associates are known (see the result from [15] cited below), it is not known how well these bounds reflect the actual behaviour of these numbers.

It would not be unreasonable to suspect that this number depends on the field \mathbb{K} . In fact, given a result of Schmidt on norm-form equations to be cited below, one might even believe that this number depends only on r .

However, we show here that this is not correct. In particular, we have the following result.

Theorem 1. *For any positive integer N and any number field \mathbb{K} with $[\mathbb{K} : \mathbb{Q}] \geq 3$, there exists a full module $\mathcal{M}_N \subseteq \mathbb{K}$ with at least N pairwise non-associates of norm 1.*

Note 1. The full modules, \mathcal{M}_N , that we construct here are not rare or exotic in structure. In fact, it will be apparent in Section 3 that they are plentiful and simply-defined – this is even more striking in Note 6 there.

Note 2. Lemma 12 shows that such a result is not true if \mathbb{K} is a quadratic extension of \mathbb{Q} .

Our construction in this paper fails for quadratic fields, as it should from Lemma 12, since at least three generators of the modules are required:

- (i) $1 \in \mathcal{M}_N$,
- (ii) a fixed unit $\epsilon \in \mathcal{M}_N$ and
- (iii) a third generator, dependent on N , must be in \mathcal{M}_N .

1.2. Norm form equations.

Definition 3. A *norm form* $F(\mathbf{X}) = F(X_1, \dots, X_n)$ is a polynomial in $\mathbb{Q}[X_1, \dots, X_n]$ that can be expressed as

$$F(\mathbf{X}) = a\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha_1 X_1 + \dots + \alpha_n X_n)$$

where a is a non-zero rational number, $\alpha_1, \dots, \alpha_n$ lie in an algebraic number field \mathbb{K} and $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}$ denotes the norm from \mathbb{K} to \mathbb{Q} .

For $i = 1, \dots, r$, we let σ_i denote the isomorphic embeddings of \mathbb{K} into \mathbb{C} and write $\alpha^{(i)} = \sigma_i(\alpha)$ for any $\alpha \in \mathbb{K}$. With $L(\mathbf{X}) = \alpha_1 X_1 + \dots + \alpha_n X_n$, as above, and $L^{(i)}(\mathbf{X}) = \alpha_1^{(i)} X_1 + \dots + \alpha_n^{(i)} X_n$ for $i = 1, \dots, r$. We can write $F(\mathbf{X})$ in the form

$$(1) \quad F(\mathbf{X}) = aL^{(1)}(\mathbf{X}) \dots L^{(r)}(\mathbf{X}).$$

Definition 4. We call two modules \mathcal{L} and \mathcal{M} proportional if there is a fixed $\sigma \neq 0$ such that $\mathcal{M} = \sigma\mathcal{L}$.

A module \mathcal{M} (and hence $F(\mathbf{X})$) is called *degenerate* if it contains a submodule \mathcal{M}_0 that is proportional to a full module \mathcal{L} in some subfield \mathbb{L} of \mathbb{K} , where \mathbb{L} is neither \mathbb{Q} nor an imaginary quadratic field.

This definition was formulated by Schmidt [9, 10] in the early 1970's and he showed that there are non-zero rational numbers m such that $F(\mathbf{X}) = m$ has infinitely many solutions in \mathbb{Z}^n if and only if F is degenerate. Moreover, he was also able to show that even if F is degenerate, then there is a notion of a family of solutions such that there are only finitely many families of solutions of $F(\mathbf{X}) = m$.

Definition 5. Suppose that $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = m$ has a solution $\alpha \in \mathcal{M}^{\mathbb{L}}$, then every element of $\alpha\mathcal{U}_{\mathcal{M}}^{\mathbb{L}}$ is also a solution and we call this set of solutions a *family* of solutions. Similarly, the set of all elements $\mathbf{x} \in \mathbb{Z}^n$ such that $L(\mathbf{x}) \in \alpha\mathcal{U}_{\mathcal{M}}^{\mathbb{L}}$ is called a *family* of solutions.

That this is a natural notion of a family of solutions is probably best seen by means of examples and so we invite the reader to consult those presented in [10, Section 3] and [11, Section VII.3].

By the end of the 1980's, Schmidt had proven his quantitative subspace theorem [12] and used it to establish upper bounds that depend only on m , n and r for the number of solutions of the norm form equation $F(\mathbf{X}) = m$ when F is non-degenerate [13].

At that time, Schmidt posed to this author the question of what sort of bounds one could obtain for the number of families of solutions of degenerate norm forms.

The author [15, Theorem V.1] obtained a bound depending only on m, n and r for the number of full submodules in subfields of \mathbb{K} such that any solution of $F(\mathbf{X}) = m$ must lie in the union of these submodules. Győry [6, Theorem 7] has independently established this same result. The most recent results in this area are due to Evertse and Győry [5]. Their results are much more general than the following, but their Theorem 1 implies that the solutions of $F(\mathbf{X}) = 1$ lie in the union of at most

$$(2^{33}r^2)^{n(n+1)(2n+1)/3-2}$$

full submodules of subfields of \mathbb{K} .

As was mentioned in the previous paragraph, Győry's work in this area has been much more general. He has generalised the concept of a family of solutions for the norm form setting to that of decomposable form equations.

Decomposable forms include not only norm forms, but also discriminant forms, index forms, resultant forms, reducible binary forms and other kinds of forms as well. Moreover, Győry considers these decomposable form equations over number fields and, more generally, over finitely generated fields.

Similar to the author's results to be cited in the next paragraph, in [5, 6], Győry obtained explicit upper bounds for the number of families which depend on certain "indices" associated with the module.

For full modules, the author could only establish bounds for the number of families of solutions which depended more closely on the given module. In particular,

Lemma V.2 of [15] states that if $\mathcal{O}_{\mathcal{M}}$ is the ring of coefficients of \mathcal{M} and $[\mathcal{U}_{\mathbb{K}} : \mathcal{U}_{\mathcal{M}}]$ is the index of the unit group of $\mathcal{O}_{\mathcal{M}}$ in the unit group of \mathbb{K} , then the solutions of the norm form equation $F(\mathbf{X}) = m$ lie in the union of at most

$$(2) \quad [\mathcal{U}_{\mathbb{K}} : \mathcal{U}_{\mathcal{M}}] \tau(|m|)^r$$

families, where τ is the function which counts the number of positive divisors of a rational integer. In Theorem V.2 of [15], an upper bound in terms of the coefficients of \mathcal{M} was obtained.

For a full module, \mathcal{M} , the number of families of solutions of the associated norm-form equation $F(\mathbf{X}) = m$ is equal to the number of non-associates in \mathcal{M} of norm m/a . Hence, from Theorem 1, we obtain the following Corollary.

Corollary 1. *For any positive integer N and any number field \mathbb{K} with $[\mathbb{K} : \mathbb{Q}] \geq 3$, there exists a full module $\mathcal{M}_N \subseteq \mathbb{K}$ such that the equation $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\mu) = 1$ has at least N families of solutions with $\mu \in \mathcal{M}_N$.*

Despite Corollary 1, for norm forms in three variables which do not arise from full modules, we are able to get a bound of the desired form. In fact, this is only possible because Corollary 1 is not true when \mathbb{K} is a quadratic field.

Theorem 2. *Let α_1, α_2 and α_3 be algebraic numbers which are linearly independent over \mathbb{Q} . Putting $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, $r = [\mathbb{K} : \mathbb{Q}]$ and $L(\mathbf{X}) = \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3$, we consider the norm form equation*

$$(3) \quad F(\mathbf{X}) = a \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = 1,$$

where a is a non-zero rational number and $F(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$.

If $[\mathbb{Q}(\alpha_2/\alpha_1, \alpha_3/\alpha_1) : \mathbb{Q}] > 3$, then the solutions of this equation lie in at most $10^{969} r^{10}$ families.

Note 3. The restriction that the α_i 's be linearly independent is no real restriction, for otherwise the norm form equation $F(\mathbf{X}) = 1$ becomes a Thue equation.

Note 4. The condition that $[\mathbb{Q}(\alpha_2/\alpha_1, \alpha_3/\alpha_1) : \mathbb{Q}] > 3$ ensures that the module generated by $L(\mathbf{X})$ is not proportional to a full module in any subfield of \mathbb{K} .

Note 5. With the exception of refinements, this work establishes this aspect of the behaviour of the number of families of solutions of norm form equations in three variables.

The method of proof of Theorem 2 fails when $F(\mathbf{X})$ is a norm form in four (or more) variables satisfying analogous conditions. By Schmidt's Subspace Theorem, all the solutions of $F(\mathbf{X}) = 1$ correspond to elements of certain three-dimensional subspaces of \mathbb{Q}^4 . If one of these subspaces gives rise to a full module of rank 3, then, from Corollary 1, it is possible for there to be an arbitrarily large number of families of solutions.

Several questions and directions for further investigation come to mind.

It would be of considerable diophantine interest to determine the nature of the dependence of the number of families of solutions on $F(\mathbf{X})$ or \mathcal{M} .

From the proof of Theorem 1, it is clear that some dependence on $[\mathcal{U}_{\mathbb{K}} : \mathcal{U}_{\mathcal{M}}]$ as in (2) is necessary.

Under what circumstances is the number of families independent of the module \mathcal{M} ?

Bombieri and Schmidt [2] have shown that $O(r)$ is the correct order of growth for the number of solutions of Thue equations. What is the correct order of growth in Theorem 2?

2. PRELIMINARY LEMMAS TO THE PROOF OF THEOREM 1

The following is Exercise 5 on page 93 of [1]. We include a proof for completeness.

Lemma 1. *Let \mathcal{M}_1 and \mathcal{M}_2 be two full \mathbb{Z} -modules in \mathbb{K} . Then $\mathcal{M}_1 \cap \mathcal{M}_2$ is a full \mathbb{Z} -module.*

Proof. Let $\{\beta_{1,1}, \dots, \beta_{1,r}\}$ and $\{\beta_{2,1}, \dots, \beta_{2,r}\}$ be sets of generators for \mathcal{M}_1 and \mathcal{M}_2 , respectively. Since these are full modules, each of these sets of generators forms a basis for \mathbb{K} as a \mathbb{Q} -vector space. Hence each $\beta_{2,i}$ can be expressed as a linear combination over \mathbb{Q} of the $\beta_{1,j}$'s. Therefore, there exist least positive integers $d_{2,i}$, such that $d_{2,i}\beta_{2,i} \in \mathcal{M}_1$. Therefore, $d_{2,i}\beta_{2,i} \in \mathcal{M}_1 \cap \mathcal{M}_2$ for each i .

Furthermore, the $d_{2,i}\beta_{2,i}$'s are linearly independent over \mathbb{Q} . Hence $\mathcal{M}_1 \cap \mathcal{M}_2$ has r generators and is a full module. \square

The next lemma is the key result in establishing Theorem 1.

Lemma 2. *Let ϵ be a unit in \mathbb{K} with norm 1 and not a root of unity. For each positive integer, i , let $\mathcal{M}^{(i)}$ be a full module in \mathbb{K} with $\mathcal{O}^{(i)}$ as its ring of coefficients and $\mathcal{U}^{(i)}$ as the units of norm 1 in $\mathcal{O}^{(i)}$. Further, let ℓ_i be the number of distinct multiplicative cosets of the form $\epsilon^v \mathcal{U}^{(i)}$.*

Suppose that:

- (a) $\mathcal{O}^{(i)}$ is a proper subset of $\mathcal{M}^{(i)}$,
- (b) ϵ is in $\mathcal{M}^{(i)}$ but not in $\mathcal{O}^{(i)}$ for each i ,
- (c) the ℓ_i 's are finite and pairwise relatively prime and all greater than 1,
- (d) $\mathcal{O}_{\bigcap_{i=1}^N \mathcal{M}^{(i)}} = \bigcap_{i=1}^N \mathcal{O}^{(i)}$, for all positive integers N .

Then, for all positive integers N , $\bigcap_{i=1}^N \mathcal{M}^{(i)}$ is a full module containing at least 2^N units which are pairwise non-associates.

Proof. From Lemma 1, it follows that $\bigcap_{i=1}^N \mathcal{M}^{(i)}$ is a full module. So it remains only to prove the statement about the units.

Let $\mathcal{S} \subseteq \{1, \dots, N\}$.

We define $a_{\mathcal{S}}$ by

$$a_{\mathcal{S}} \equiv \begin{cases} 0 \bmod \ell_i & \text{if } i \in \mathcal{S} \\ 1 \bmod \ell_i & \text{if } i \notin \mathcal{S} \end{cases}$$

for each $1 \leq i \leq N$.

By condition (b), $\epsilon \notin \mathcal{O}^{(i)}$, so it follows that $\ell_i > 1$.

By condition (c), the ℓ_i 's are relatively prime, so we can find such an $a_{\mathcal{S}}$ from the Chinese Remainder Theorem.

Next note that if $i \in \mathcal{S}$, then $\epsilon^{a_{\mathcal{S}}} \in \mathcal{U}^{(i)} \subseteq \mathcal{O}^{(i)} \subseteq \mathcal{M}^{(i)}$, by condition (a).

If $i \notin \mathcal{S}$, then $\epsilon^{a_{\mathcal{S}}-1} \in \mathcal{U}^{(i)} \subseteq \mathcal{O}^{(i)}$. Since $\epsilon \in \mathcal{M}^{(i)}$, once again $\epsilon^{a_{\mathcal{S}}} = \epsilon^{a_{\mathcal{S}}-1} \cdot \epsilon \in \mathcal{M}^{(i)}$.

Hence $\epsilon^{a_{\mathcal{S}}} \in \bigcap_{i=1}^N \mathcal{M}^{(i)}$ for each \mathcal{S} .

However, if $\mathcal{S} \neq \mathcal{S}'$ are two distinct subsets of $\{1, \dots, N\}$, then, without loss of generality, there is an $i \in \mathcal{S}$ such that $i \notin \mathcal{S}'$. Therefore, $\epsilon^{a_{\mathcal{S}}} / \epsilon^{a_{\mathcal{S}'}} \notin \mathcal{U}^{(i)}$ and hence $\epsilon^{a_{\mathcal{S}}} / \epsilon^{a_{\mathcal{S}'}} \notin \bigcap_{i=1}^N \mathcal{U}^{(i)}$.

Since there are 2^N distinct subsets, \mathcal{S} , there are at least 2^N such units.

Furthermore, by condition (d), $\mathcal{O}_{\bigcap_{i=1}^N \mathcal{M}^{(i)}} = \bigcap_{i=1}^N \mathcal{O}^{(i)}$, so $\mathcal{U}_{\bigcap_{i=1}^N \mathcal{M}^{(i)}} = \bigcap_{i=1}^N \mathcal{U}^{(i)}$

and so these units are non-associates in $\bigcap_{i=1}^N \mathcal{M}^{(i)}$. \square

Now we provide some results about the sorts of full modules that we will use to construct our examples. We start with our definition and notation for them.

Definition 6. Suppose that α_1 is an algebraic integer of degree r_1 over \mathbb{Q} , that α_2 is of degree r_2 over $\mathbb{Q}(\alpha_1)$ and that the minimal polynomial of α_2 over $\mathbb{Z}[\alpha_1]$ is monic. We let $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2)$.

For any positive integer n , let $\mathcal{M}_n(\alpha_1, \alpha_2)$ be the \mathbb{Z} -module in \mathbb{K} generated by $\left\{ \alpha_1^i \alpha_2^j : 0 \leq i \leq r_1 - 1, 0 \leq j \leq r_2 - 1 \text{ with } (i, j) \neq (r_1 - 1, r_2 - 1) \right\}$ and $n\alpha_1^{r_1-1}\alpha_2^{r_2-1}$.

$\mathcal{M}_n(\alpha_1, \alpha_2)$ is a full module in \mathbb{K} , so $\mathcal{M}_n(\alpha_1, \alpha_2)^{\mathbb{K}} = \mathcal{M}_n(\alpha_1, \alpha_2)$ and we can unambiguously denote $\mathcal{O}_{\mathcal{M}_n(\alpha_1, \alpha_2)}^{\mathbb{K}}$ by $\mathcal{O}_n(\alpha_1, \alpha_2)$.

Lemma 3. (i) $\mathcal{O}_n(\alpha_1, \alpha_2)$ is the order generated as a \mathbb{Z} -module by 1 and $\left\{ n\alpha_1^i \alpha_2^j \right\}_{0 \leq i \leq r_1-1, 0 \leq j \leq r_2-1}$ where i and j are not both 0.

(ii) Let k_1, \dots, k_N be positive integers with K_N as their least common multiple.

Then

$$\bigcap_{i=1}^N \mathcal{M}_{k_i}(\alpha_1, \alpha_2) = \mathcal{M}_{K_N}(\alpha_1, \alpha_2)$$

and

$$\bigcap_{i=1}^N \mathcal{O}_{k_i}(\alpha_1, \alpha_2) = \mathcal{O}_{K_N}(\alpha_1, \alpha_2).$$

Proof. (i) First observe that $1 \in \mathcal{O}_n(\alpha_1, \alpha_2)$.

Since $\mathcal{O}_n(\alpha_1, \alpha_2) \subseteq \mathbb{K}$, we can write any element of $\mathcal{O}_n(\alpha_1, \alpha_2)$ as $\sum_{i,j} b_{i,j} \alpha_1^i \alpha_2^j$ with $b_{i,j} \in \mathbb{Q}$.

Suppose $\sum_{i,j} b_{i,j} \alpha_1^i \alpha_2^j \in \mathcal{O}_n(\alpha_1, \alpha_2)$ and arrange the terms so that the pairs (i, j) are ordered lexicographically (i.e., (i_1, j_1) is before (i_2, j_2) if $i_1 < i_2$ or if $i_1 = i_2$ and $j_1 < j_2$). Let (i_0, j_0) be the last pair such that $b_{i,j} \not\equiv 0 \pmod{n}$.

If $(i_0, j_0) = (0, 0)$, then since $b_{0,0} \cdot 1 \in \mathcal{M}_n(\alpha_1, \alpha_2)$, we must have $b_{0,0} \in \mathbb{Z}$.

If $(i_0, j_0) \neq (0, 0)$, then $\left(\sum_{i,j} b_{i,j} \alpha_1^i \alpha_2^j\right) \cdot \left(\alpha_1^{r_1-1-i_0} \alpha_2^{r_2-1-j_0}\right) = b_{i_0,j_0} \alpha_1^{r_1-1} \alpha_2^{r_2-1}$ plus an element of the form $n\mathcal{M}_1(\alpha_1, \alpha_2)$ (i.e., in $\mathcal{M}_n(\alpha_1, \alpha_2)$) plus “smaller” terms lexicographically. This product is also in $\mathcal{M}_n(\alpha_1, \alpha_2)$ and since $\{\alpha_1^i \alpha_2^j\}_{0 \leq i \leq r_1-1, 0 \leq j \leq r_2-1}$ form a basis of \mathbb{K} so this product has a unique representation of terms of this basis, we see that $n|b_{i_0,j_0}$.

Proceeding inductively, it follows that $\mathcal{O}_n(\alpha_1, \alpha_2)$ is contained in the order generated by 1 and $\{n\alpha_1^i \alpha_2^j\}_{0 \leq i \leq r_1-1, 0 \leq j \leq r_2-1}$ where i and j are not both 0.

Since the minimal polynomial of α_2 over $\mathbb{Z}[\alpha_1]$ is monic, it is immediate that $n\alpha_1^i \alpha_2^j \mathcal{M}_n(\alpha_1, \alpha_2) \subseteq n\mathcal{M}_1(\alpha_1, \alpha_2) \subseteq \mathcal{M}_n(\alpha_1, \alpha_2)$ and so (i) follows.

(ii) We prove here a more general result from which both statements follow.

Let S be any subset of ordered pairs of the form (i, j) with $0 \leq i \leq r_1 - 1$ and $0 \leq j \leq r_2 - 1$. Define $\mathcal{M}_{n,S}(\alpha_1, \alpha_2)$ to be the full module generated by $\{\alpha_1^i \alpha_2^j\}_{(i,j) \notin S}$ and $\{n\alpha_1^i \alpha_2^j\}_{(i,j) \in S}$.

We prove that

$$\bigcap_{i=1}^N \mathcal{M}_{k_i,S}(\alpha_1, \alpha_2) = \mathcal{M}_{K_N,S}(\alpha_1, \alpha_2).$$

Note that we need only prove this for $N = 2$ as it follows in general, by induction on N .

Suppose that $\beta \in \mathcal{M}_{k_1,S}(\alpha_1, \alpha_2) \cap \mathcal{M}_{k_2,S}(\alpha_1, \alpha_2)$. Then

$$\beta = \sum_{(i,j) \notin S} a_{i,j} \alpha_1^i \alpha_2^j + \sum_{(i,j) \in S} a_{i,j} k_1 \alpha_1^i \alpha_2^j = \sum_{(i,j) \notin S} b_{i,j} \alpha_1^i \alpha_2^j + \sum_{(i,j) \in S} b_{i,j} k_2 \alpha_1^i \alpha_2^j,$$

where the $a_{i,j}$ ’s and the $b_{i,j}$ ’s are integers.

Since β has a unique representation as a linear combination of the $\alpha_1^i \alpha_2^j$ ’s with rational coefficients, it must be the case that $a_{i,j} = b_{i,j}$ for $(i, j) \notin S$ and that $a_{i,j} k_1 = b_{i,j} k_2$ for $(i, j) \in S$. Hence, k_2 is a divisor of $a_{i,j} k_1$ for $(i, j) \in S$, that is $a_{i,j} k_1 = a'_{i,j} \text{lcm}(k_1, k_2)$ for $(i, j) \in S$.

Thus $\beta \in \mathcal{M}_{K_2,S}(\alpha_1, \alpha_2)$ and so $\mathcal{M}_{k_1,S}(\alpha_1, \alpha_2) \cap \mathcal{M}_{k_2,S}(\alpha_1, \alpha_2) \subseteq \mathcal{M}_{K_2,S}(\alpha_1, \alpha_2)$.

Now we prove the other inclusion. Suppose that $\beta \in \mathcal{M}_{K_2, S}(\alpha_1, \alpha_2)$. Then

$$\beta = \sum_{(i,j) \notin S} a_{i,j} \alpha_1^i \alpha_2^j + \sum_{(i,j) \in S} a_{i,j} K_2 \alpha_1^i \alpha_2^j,$$

where the $a_{i,j}$'s are integers and hence k_1, k_2 both divide all of $K_2 a_{i,j}$ for $(i, j) \in S$. Therefore, $\beta \in \mathcal{M}_{k_1, S}(\alpha_1, \alpha_2) \cap \mathcal{M}_{k_2, S}(\alpha_1, \alpha_2)$, so

$$\mathcal{M}_{K_2, S}(\alpha_1, \alpha_2) \subseteq \mathcal{M}_{k_1, S}(\alpha_1, \alpha_2) \cap \mathcal{M}_{k_2, S}(\alpha_1, \alpha_2).$$

Together, these set inclusions show that

$$\mathcal{M}_{k_1, S}(\alpha_1, \alpha_2) \cap \mathcal{M}_{k_2, S}(\alpha_1, \alpha_2) = \mathcal{M}_{K_2, S}(\alpha_1, \alpha_2).$$

The result for the $\mathcal{M}_{k_i}(\alpha_1, \alpha_2)$'s holds by putting $S = (r_1 - 1, r_2 - 1)$, while the result for the $\mathcal{O}_{k_i}(\alpha_1, \alpha_2)$'s holds by putting $S = \{(i, j) : 0 \leq i \leq r_1 - 1, 0 \leq j \leq r_2 - 1\} - (0, 0)$. \square

Lemma 4. *Let r be a positive integer and put $g_r(X) = \prod_{i=1}^r (X^i - 1)$.*

There exist positive integers m_r , n_r and s_r with $\gcd(m_r, s_r) = 1$ such that the following hold.

- (i) $g_r(x)/n_r \in \mathbb{Z}$ for all $x \in \mathbb{Z}$ with $x \equiv s_r \pmod{m_r}$.
- (ii) *There exists an infinite sequence of primes $\{p_{r,i}\}$ satisfying $p_{r,i} \equiv s_r \pmod{m_r}$ for all i and such that the numbers $g_r(p_{r,i})/n_r$ ($i = 1, 2, \dots$), are pairwise relatively prime integers each greater than 1.*

Proof. (i) Let p be the least prime number greater than $r + 1$, set $n_r = g_r(p)$ and $m_r = n_r(r + 1)!$. Note that $n_r = g_r(p) \neq 0$, so we can divide by n_r in what follows.

For all $x \equiv p \pmod{m_r}$, $g_r(x) \equiv g_r(p) \equiv n_r \pmod{m_r}$. Since m_r is a multiple of n_r , $g_r(x)/n_r$ is an integer for such x . Hence we let $s_r = p$.

(ii) Notice that p in the proof of part (i) does not divide n_r , since p does not divide $p^j - 1$ for any $j > 0$. In addition, $p > r + 1$, so p cannot divide $(r + 1)!$. Together, these two statements imply that p cannot divide m_r . Therefore, there are infinitely many primes congruent to $p \pmod{m_r}$, that is $s_r \pmod{m_r}$. Among all such primes, we must show that there are infinitely many such that $g_r(p_{r,i})/n_r$ are pairwise relatively prime. We define such a collection of primes inductively.

First, let $p_{r,1}$ be the smallest prime congruent to $s_r \pmod{m_r}$ such that all the real roots of $g_r(X)/n_r - 1$ are less than $p_{r,1}$.

Next suppose that we have a set of primes $p_{r,1}, \dots, p_{r,N}$ that satisfy the conditions in the lemma.

We now find a prime $p_{r,N+1}$ such that $p_{r,1}, \dots, p_{r,N+1}$ satisfy the conditions in the lemma.

Let \mathcal{P}_N be the set of all primes that divide

$$\Pi_N = \prod_{i=1}^N \frac{g_r(p_{r,i})}{n_r}.$$

Let $q \in \mathcal{P}_N$.

Since $g_r(p_{r,i}) \equiv g_r(s_r) \equiv g_r(p) \equiv n_r \pmod{m_r}$ for $p_{r,i} \equiv s_r \pmod{m_r}$, $g_r(p_{r,i})/n_r \equiv 1 \pmod{(r+1)!}$. So $\gcd(g_r(p_{r,i})/n_r, (r+1)!) = 1$. Hence $q > r+1$ or, more conveniently for what follows, $q-1 \geq r+1$.

Now the zeroes of $g_r(X) \pmod{q}$ are the roots of unity \pmod{q} of order at most r . Since q is prime, there always exists a primitive root, b_q , modulo q , i.e., a number b_q such that $b_q^{q-1} \equiv 1 \pmod{q}$ and $b_q^k \not\equiv 1 \pmod{q}$ for $0 < k < q-1$. Therefore, b_q is a primitive $q-1$ -st root of unity \pmod{q} . Now since $q-1 \geq r+1$, $g_r(b_q) \not\equiv 0 \pmod{q}$. Therefore, for each $q \in \mathcal{P}_N$, there is a non-zero congruence class, b_q , such that $g_r(b_q) \not\equiv 0 \pmod{q}$.

We choose $p_{r,N+1}$ to be a prime satisfying $p_{r,N+1} > p_{r,N}$, $p_{r,N+1} \equiv s_r \pmod{m_r}$ and $p_{r,N+1} \equiv b_q \pmod{q}$ for each $q \in \mathcal{P}_N$. From this last condition, we have $g_r(p_{r,N+1}) \not\equiv 0 \pmod{q}$ for any $q \in \mathcal{P}_N$. By Dirichlet's theorem on primes in arithmetic progressions, there does exist such a $p_{r,N+1}$ (in fact, there are infinitely many such primes).

Finally, suppose that p' is a prime which divides $g_r(p_{r,N+1})/n_r$. Then $g_r(p_{r,N+1}) \equiv 0 \pmod{p'}$ and thus $p' \notin \mathcal{P}_N$. This shows that $g_r(p_{r,N+1})/n_r$ and Π_N are relatively prime as desired.

Furthermore, since $p_{r,N} > p_{r,1}$ for all $N \geq 2$ and $p_{r,1}$ is larger than all the real roots of $g_r(X)/n_r - 1$, our condition that $g_r(p_{r,N})/n_r > 1$ also holds. \square

Lemma 5. *Let \mathbb{K} a number field with $r = [\mathbb{K} : \mathbb{Q}] \geq 2$ containing an order \mathcal{O} . For any positive integer n , let \mathcal{O}_n be the order generated as a \mathbb{Z} -module by 1 and $n\mathcal{O}$. Let $\eta \in \mathcal{O}$ be a unit of norm 1 and not a root of unity. Put $\epsilon = \eta^{n_r}$, using the notation of Lemma 4. For any prime p satisfying $p \equiv s_r \pmod{m_r}$ which does not divide $\text{disc}(\mathcal{O})$, let t be the least positive integer such that $\epsilon^t \in \mathcal{O}_p$. Then t divides $g_r(p)/n_r$.*

Proof. First recall from Lemma 4(i) that $g_r(p)/n_r$ is an integer.

The discriminant of \mathbb{K} is a divisor of $\text{disc}(\mathcal{O})$ and, by assumption, p is not a divisor of $\text{disc}(\mathcal{O})$. Therefore p does not ramify in \mathbb{K} and we have

$$(4) \quad \mathcal{O}_{\mathbb{K}}/(p) \cong \mathcal{O}_{\mathbb{K}}/P_1 \times \cdots \times \mathcal{O}_{\mathbb{K}}/P_s$$

via the map that takes $x + (p)$ to $(x + P_1, \dots, x + P_s)$ (see Theorem 2, p. 111 of [8]), where the P_i 's are prime ideals in $\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}_{\mathbb{K}}/P_i$ is a field of cardinality p^{f_i} and $f_1 + \cdots + f_s = r$. The right-hand side of (4) is a ring under term-wise addition and multiplication.

Since η is a unit, $\eta + P_i \neq 0 + P_i$. Hence $(\eta + P_i)^{p^{f_i}-1} = 1 + P_i$ for each $i = 1, \dots, s$.

Let $F = \text{lcm}(p^{f_1} - 1, \dots, p^{f_s} - 1)$. Then $\eta^F \equiv 1 \pmod{p}$. Now since $F|g_r(p)$, it follows that $\eta^{g_r(p)} \equiv 1 \pmod{p}$, which is to say that there exists $\gamma \in \mathcal{O}_{\mathbb{K}}$ such that $\eta^{g_r(p)} = \epsilon^{g_r(p)/n_r} = 1 + p\gamma$.

Letting $\alpha_1, \dots, \alpha_r$ be a basis for \mathcal{O} over \mathbb{Z} , we can write

$$\gamma = \frac{a_1\alpha_1 + a_2\alpha_2 + \dots + a_r\alpha_r}{\text{disc}(\mathcal{O})},$$

where $a_1, \dots, a_r \in \mathbb{Z}$ (see Theorem 9 on page 29 of [7]).

Since $\epsilon^{g_r(p)/n_r} \in \mathcal{O}$, we can write

$$\epsilon^{g_r(p)/n_r} = 1 + \frac{pa_1\alpha_1}{\text{disc}(\mathcal{O})} + \dots + \frac{pa_r\alpha_r}{\text{disc}(\mathcal{O})} = b_1\alpha_1 + \dots + b_r\alpha_r,$$

where $b_1, \dots, b_r \in \mathbb{Z}$.

Any such representation must also be unique, since the α_i 's form a basis for \mathcal{O} , so we must have $pa_1/\text{disc}(\mathcal{O}), \dots, pa_r/\text{disc}(\mathcal{O}) \in \mathbb{Z}$. Since, by hypothesis, $p \nmid \text{disc}(\mathcal{O})$, $a'_i = a_i/\text{disc}(\mathcal{O}) \in \mathbb{Z}$ for each i . Therefore, $\epsilon^{g_r(p)/n_r} = 1 + pa'_1\alpha_1 + \dots + pa'_r\alpha_r \in \mathcal{O}_p$.

The cosets of the form $\epsilon^v \mathcal{U}_p$, where \mathcal{U}_p is the group of units of norm 1 in \mathcal{O}_p , form a group under multiplication. So if $\epsilon^t \in \mathcal{U}_p$, then t must be a divisor of $g_r(p)/n_r$, as desired. \square

3. PROOF OF THEOREM 1

Let \mathbb{K} be a number field with $r = [\mathbb{K} : \mathbb{Q}] \geq 3$ and let η be a unit in \mathbb{K} of norm 1 which is not a root of unity. Put $\epsilon = \eta^{n_r}$, where n_r is as in Lemma 4. Let α be a primitive element of the extension $\mathbb{K}/\mathbb{Q}(\epsilon)$ whose minimal polynomial over $\mathbb{Z}[\epsilon]$ is monic (with $\alpha = 1$ if $\mathbb{K} = \mathbb{Q}(\epsilon)$).

For any positive integer N , let $k_1 = p_{r,1}, \dots, k_N = p_{r,N}$ be the first N elements of a sequence of primes satisfying the conditions in Lemmas 4 and 5 (with $\mathcal{O} = \mathcal{M}_1(\epsilon, \alpha)$ – note that this is an order in \mathbb{K} by our conditions on α). Put $K_N = k_1 \cdots k_N$.

We are now ready to apply Lemma 2 to prove Theorem 1.

We let $\mathcal{M}^{(i)} = \mathcal{M}_{k_i}(\epsilon, \alpha)$, so that $\mathcal{O}^{(i)} = \mathcal{O}_{k_i}(\epsilon, \alpha)$ from Lemma 3(i).

Notice that $\mathcal{O}^{(i)}$ is a proper subset of $\mathcal{M}^{(i)}$, so condition (a) of Lemma 2 holds.

Also $\epsilon \in \mathcal{M}^{(i)}$ and $\epsilon \notin \mathcal{O}^{(i)}$, so condition (b) of Lemma 2 holds.

Recall from the statement of Lemma 2 that ℓ_i is the number of distinct multiplicative cosets of the form $\epsilon^v \mathcal{U}^{(i)}$, where $\mathcal{U}^{(i)}$ is the group of units of norm 1 in $\mathcal{O}^{(i)}$. From Lemmas 4(ii) and 5, we know that $\ell_i \mid (g_r(k_i)/n_r)$, which are all pairwise relatively prime and that $\ell_i > 1$. Therefore, condition (c) of Lemma 2 holds.

Finally, from Lemma 3(ii), condition (d) of Lemma 2 holds.

Since all the conditions in Lemma 2 are satisfied, $\mathcal{M}_{K_N}(\epsilon, \alpha) = \bigcap_{i=1}^N \mathcal{M}_{k_i}(\epsilon, \alpha)$ (equality holding by Lemma 3(ii)) has at least 2^N units that are non-associates.

Hence Theorem 1 holds.

Note 6. These modules, $\mathcal{M}_n(\alpha, \epsilon)$, are in fact special cases of more general examples.

Let \mathcal{O} be any order in \mathbb{K} , η any unit in \mathcal{O} of norm 1 which is not a root of unity and put $\epsilon = \eta^{nr}$. Let $\varphi : \mathcal{O} \rightarrow \mathbb{Z}$ be any non-trivial \mathbb{Z} -module homomorphism such that $\varphi(1) = \varphi(\epsilon) = 0$. Define $\mathcal{M}_{n,\epsilon,\varphi}$ to be the kernel of the map $\varphi \bmod n$ from \mathcal{O} to $\mathbb{Z}/n\mathbb{Z}$. It is a full module in \mathbb{K} .

If n is relatively prime to $\det(\varphi(\omega_i\omega_j))$, where $\{\omega_i\}$ is a basis for \mathcal{O} as a \mathbb{Z} -module (and the value of this determinant is, in fact, independent of the choice of basis of \mathcal{O}), then $\mathcal{O}_{n,\epsilon,\varphi}$, the ring of coefficients of $\mathcal{M}_{n,\epsilon,\varphi}$, is $\mathbb{Z} + n\mathcal{O}$.

Thus the other lemmas in this section can be applied, as here, to construct modules from these $\mathcal{M}_{n,\epsilon,\varphi}$'s with arbitrarily many units that are non-associates.

4. PRELIMINARY LEMMAS TO THE PROOF OF THEOREM 2

Lemma 6. *Given $\alpha_1, \dots, \alpha_n$ which are \mathbb{Q} -linearly independent elements of a number field \mathbb{K} , let \mathcal{M} be the \mathbb{Z} -module generated by these α_i 's. If n is prime and \mathbb{L} is a number field such that $\mathcal{M}^{\mathbb{L}} = \mathcal{M}$ then either \mathcal{M} is proportional to a full module in \mathbb{L} or $\mathbb{L} = \mathbb{Q}$.*

Proof. Let $\mathcal{M}\mathbb{L}$ be the set of all products of the form $\alpha\mu$ where $\alpha \in \mathbb{L}$ and $\mu \in \mathcal{M}$. It is easy to see that $\mathcal{M}\mathbb{L}$ is closed under multiplication by elements of \mathbb{L} . Suppose that $\alpha\mu_1, \beta\mu_2 \in \mathcal{M}\mathbb{L}$. Since $\mathcal{M}^{\mathbb{L}} = \mathcal{M}$, there is a non-zero rational integer a such that $a(\alpha\mu_1 + \beta\mu_2) \in \mathcal{M}$. Thus $\alpha\mu_1 + \beta\mu_2 \in \mathcal{M}\mathbb{L}$. So $\mathcal{M}\mathbb{L}$ is also closed under addition and hence is a vector space over \mathbb{L} of dimension d , say.

Since $\mathcal{M}^{\mathbb{L}} = \mathcal{M}$, we have $\mathcal{M}\mathbb{L} = \mathcal{M}\mathbb{Q}$ and hence $\dim_{\mathbb{Q}}(\mathcal{M}\mathbb{Q}) = d[\mathbb{L} : \mathbb{Q}] = n$. However, n is prime so either $d = 1$, in which case \mathcal{M} is proportional to a full module in \mathbb{L} , or $[\mathbb{L} : \mathbb{Q}] = 1$ so that $\mathbb{L} = \mathbb{Q}$. \square

In the case of our theorem, i.e., $n = 3$ and $r = [\mathbb{K} : \mathbb{Q}] > 3$, Lemma 6 tells us that if $\mathcal{M}^{\mathbb{L}} = \mathcal{M}$ then $\mathbb{L} = \mathbb{Q}$. This information turns out to be crucial in what follows.

We will use the heights $H(\cdot)$, $H^*(\cdot)$ and $\mathcal{H}(\cdot)$ defined on pages 201 and 204 of [13]. Let $L = \sum_{j=1}^n \alpha_j X_j$ be a linear form with coefficients in an algebraic number field \mathbb{K} of degree r over \mathbb{Q} and let $a \in \mathbb{Q}^*$ be such that the norm form

$$F(\mathbf{X}) = a\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = a \prod_{i=1}^r \left(\sum_{j=1}^n \alpha_j^{(i)} X_j \right)$$

has its coefficients in \mathbb{Z} . Then the height of F , $H^*(F)$, is defined by

$$H^*(F) = |a| \prod_{i=1}^r \left(\sum_{j=1}^n |\alpha_j^{(i)}|^2 \right)^{1/2}.$$

According to Lemma 1 of [13], for the absolute height $H(L)$ of the linear form L , we have

$$H^*(F) = \text{cont}(F)H(L)^r,$$

where $\text{cont}(F)$ denotes the greatest common divisor of the coefficients of F .

Two norm forms F, G are called *equivalent*, which we denote by $F \sim G$, if $G(\mathbf{X}) = F(B\mathbf{X})$ for some matrix $B \in \text{SL}(n, \mathbb{Z})$. Now $H^*(\cdot)$ is not an invariant under this equivalence, so we define an invariant height of a norm form F , $\mathcal{H}(F)$, by $\mathcal{H}(F) := \min_{G \sim F} H^*(G)$, where the minimum is taken over all norm forms G equivalent to F .

To proceed, we now divide the solutions of (3) into large and small solutions and “jack up the height” of the norm form $F(\mathbf{X})$. The point of this last process, which will be explained shortly, is to replace $F(\mathbf{X})$ by a finite number of other norm forms $F_j(\mathbf{X})$ which are of sufficiently large height so that we can apply known diophantine techniques to obtain an upper bound on the number of solutions or, when it works for degenerate norm form equations, families of solutions of $F_j(\mathbf{X}) = 1$. We create these new forms in such a way, via linear maps, that the number of solutions (or families of solutions) to the norm form equation $F(\mathbf{X}) = 1$ is at most the sum of the number of solutions (or families of solutions) of each of the norm form equations $F_j(\mathbf{X}) = 1$. Since we know the number of such norm forms, we can bound the number of solutions of $F(\mathbf{X}) = 1$.

For a prime p , let

$$A_0 = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad A_j = \begin{pmatrix} 0 & -1 \\ p & -j \end{pmatrix} \text{ for } j = 1, \dots, p.$$

For any $n \geq 2$, we let E be the $(n-2) \times (n-2)$ identity matrix and consider the $n \times n$ matrices

$$B_j = \begin{pmatrix} A_j & 0 \\ 0 & E \end{pmatrix} \text{ for } j = 0, \dots, p.$$

We can use the linear maps induced by these matrices to express

$$\mathbb{Z}^n = \bigcup_{j=0}^p B_j \mathbb{Z}^n.$$

For $j = 0, \dots, p$, we put

$$F_j(\mathbf{X}) = F(B_j \mathbf{X})$$

and notice that we can express $F_j(\mathbf{X})$ in the form

$$F_j(\mathbf{X}) = a_j \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(L_j(\mathbf{X})),$$

where a_j is a non-zero rational number and $L_j(\mathbf{X}) = L(B_j \mathbf{X})$.

Moreover, we shall assume that these $F_j(\mathbf{X})$'s are *reduced*, that is, $\mathcal{H}(F_j) = H^*(F_j)$. This idea comes from [13, p. 208] where it is noted that the number of solutions is unaffected by such an assumption.

If we let $p = 125000^3 + 21$ (which is prime), then

$$(5) \quad H(L_j) = \mathcal{H}(F_j)^{1/r} \geq p^{1/3} > 125000,$$

for each $j = 0, \dots, p$, by equations (5.3) and (5.5) of [13].

In what follows, we shall drop the subscripts on the F_j 's and L_j 's in order to simplify our notation. It is also at this point where we introduce our definition of small and large solutions.

Definition 7. We define a *small solution* of $F(\mathbf{x}) = 1$ to be one with

$$(6) \quad |\mathbf{x}| \leq H(L)^{6^{49}r^3},$$

where $|\mathbf{x}|$ denotes the ordinary Euclidean absolute value. A *large solution* will be one for which (6) does not hold.

To be able to estimate the number of small solutions we need the following lemma.

Lemma 7. *Suppose that $F(\mathbf{X})$ is a norm form as in Theorem 2 which is reduced and satisfies (5) and that $\mathbf{x} \in \mathbb{Z}^3$ is a solution of $F(\mathbf{x}) = 1$. There are three linearly independent forms $L_1(\mathbf{X}), L_2(\mathbf{X})$ and $L_3(\mathbf{X})$ with real coefficients and*

$$(7) \quad |L_1(\mathbf{x})L_2(\mathbf{x})L_3(\mathbf{x})| < |\det(L_1, L_2, L_3)| H(L)^{-2/3},$$

where $\det(L_1, L_2, L_3)$ is the determinant of the coefficient matrix.

Proof. From equation (6.1) in [13] applied with $n = 3$, there exist such linear forms with

$$\begin{aligned} |L_1(\mathbf{x})L_2(\mathbf{x})L_3(\mathbf{x})| &< \frac{8^3}{(3!)^{1/2}V(3)} |\det(L_1, L_2, L_3)| \mathcal{H}(F)^{-1/r} \\ &< 50 |\det(L_1, L_2, L_3)| \mathcal{H}(F)^{-1/r}, \end{aligned}$$

since, $V(3)$, the volume of the unit ball in \mathbb{R}^3 , is $4\pi/3$.

Note that, as in Section 6 of [13], L and its conjugate linear forms do not necessarily have real coefficients. However, as there, the procedure in [12, Section 2] can be applied to obtain the $L_1(\mathbf{X}), L_2(\mathbf{X})$ and $L_3(\mathbf{X})$ required here.

Since we have assumed that F is reduced, we know that $\mathcal{H}(F)^{1/r} = H(L)$. By the inequalities in (5), we know that $50/H(L) < 1/H(L)^{2/3}$ and the lemma follows. \square

Lemma 8. *Suppose that $F(\mathbf{X})$ is a reduced norm form as in Theorem 2 which satisfies (5). The small solutions of $F(\mathbf{x}) = 1$ lie in the union of not more than $2^{95}3^{108}r^9$ proper linear subspaces of \mathbb{Q}^3 .*

Proof. Putting $B = H(L)^{6^{49}r^3}$, $P = H(L)^{2/3}$ and $Q = (\log B)/(\log P) = 2^{48}3^{50}r^3$, we have $P = H(L)^{2/3} > 2500 > 1296 = (3!)^4$, so we can apply Schmidt's explicit version of the gap principle [12, Lemma 3.1] to (7) to show that for any choice of $L_1(\mathbf{X}), L_2(\mathbf{X})$ and $L_3(\mathbf{X})$ the solutions of (7) lie at most $2^{96}3^{109}r^6$ proper linear subspaces of \mathbb{Q}^3 .

These $L_i(\mathbf{X})$'s are obtained from the $L^{(i)}(\mathbf{X})$'s and so there are $\binom{r}{3}$ different ways of choosing them. Consideration of all these choices leads to the proof of the lemma. \square

Let us now turn to the large solutions.

We first normalise the $L^{(i)}(\mathbf{X})$'s: put $M_i(\mathbf{X}) = |L^{(i)}|^{-1} L^{(i)}(\mathbf{X})$ for $i = 1, \dots, r$.

Lemma 9. *Suppose that $F(\mathbf{X})$ is a reduced norm form as in Theorem 2 which satisfies (5) and that \mathbf{x} is a large solution of $F(\mathbf{x}) = 1$. There are integers $1 \leq i_1 < i_2 < i_3 \leq r$ such that*

$$(8) \quad |M_{i_1}(\mathbf{x})M_{i_2}(\mathbf{x})M_{i_3}(\mathbf{x})| < |\det(M_{i_1}, M_{i_2}, M_{i_3})| |\mathbf{x}|^{-1/(2 \cdot 6^{48})}.$$

Proof. By Lemma 5 of [3], $H(L) \geq \Delta_{\mathbb{K}}^{1/(2r(r-1))}$ where $[\mathbb{K} : \mathbb{Q}] = r$ and $\Delta_{\mathbb{K}}$ denotes the absolute value of the discriminant of \mathbb{K} . From Minkowski's theorem (see Corollary 3 on page 137 of [7]), we know that $\Delta_{\mathbb{K}} \geq 2$. Therefore, $H(L)^{10r^2} \geq 32 > 27$ and so, from (6), $|\mathbf{x}| > H(L)^{12r^3+10r^2} > 27H(L)^{12r^3}$, since \mathbf{x} is a large solution of (3).

Taking $\eta = r(2n)^{-n2^{n+1}}$, which is admissible by Lemma 7(ii) of [13], and $n = 3$, it follows from Lemma 8 of [13] that for every solution \mathbf{x} of (3) with $|\mathbf{x}| > 27H(L)^{12r^3}$ there are indices $1 \leq i_1 < i_2 < i_3 \leq r$ such that

$$(9) \quad |M_{i_1}(\mathbf{x})M_{i_2}(\mathbf{x})M_{i_3}(\mathbf{x})| < |\mathbf{x}|^{-1/6^{48}}.$$

In fact, Schmidt [13] proved his Lemma 8 under the assumption that the norm form under consideration is non-degenerate. However, this assumption was not used in the proof, therefore the lemma, and hence the inequality, applies as well to degenerate norm forms.

Let \mathbb{L} be the field defined by the property that a subfield \mathbb{F} of \mathbb{K} has $\mathcal{M}^{\mathbb{F}} = \mathcal{M}$ if and only if $\mathbb{F} \subset \mathbb{L}$. The only place where non-degeneracy is used in the proof of Lemma 8 of [13] is on p.214 where it is required that \mathbb{L} is either \mathbb{Q} or an imaginary quadratic field.

However, we concluded from Lemma 6 that $\mathbb{L} = \mathbb{Q}$ in our application here and hence the proof of Lemma 8 of [13] is also valid here.

By (5.3) of [12],

$$|\det(M_{i_1}, M_{i_2}, M_{i_3})| \geq H(L)^{-3r^3},$$

so that,

$$\begin{aligned} |M_{i_1}(\mathbf{x})M_{i_2}(\mathbf{x})M_{i_3}(\mathbf{x})| &< |\det(M_{i_1}, M_{i_2}, M_{i_3})| H(L)^{3r^3} |\mathbf{x}|^{-1/6^{48}} \\ &< |\det(M_{i_1}, M_{i_2}, M_{i_3})| |\mathbf{x}|^{-1/(2 \cdot 6^{48})}, \end{aligned}$$

by our definition of large solutions and (9). \square

Note 7. It is the lower bound for the determinant in the proof of this lemma, in particular the exponent on $H(L)$, which dictates our definitions of small and large solutions. This definition, in turns, affects the number of subspaces in which the solutions of our norm form equation can belong. Therefore, an improved lower bound for this determinant would lead to an improvement in Theorem 2. However, Evertse [4] has shown that in general this bound is best possible with respect to

the exponent on $H(L)$. Hence Theorem 2 seems to be the limit of this method in terms of the dependence on r .

To count the families of large solutions, Schmidt used his quantitative subspace theorem [12]. Here we shall use Evertse's refinement of this result.

Lemma 10. *Let L_1, \dots, L_n be linearly independent linear forms in n variables such that the field formed by adjoining the coefficients of any of the L_i 's to \mathbb{Q} is of degree at most D over \mathbb{Q} and $H(L_i) \leq H$. For every δ with $0 < \delta < 1$ there are proper linear subspaces $\mathcal{L}_1, \dots, \mathcal{L}_t$ of \mathbb{Q}^n with*

$$t \leq 2^{60n^2} \delta^{-7n} \log(4D) \log \log(4D)$$

such that every solution $\mathbf{x} \in \mathbb{Z}^n$ of

$$(10) \quad |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\det(L_1, \dots, L_n)| |\mathbf{x}|^{-\delta}$$

with $\gcd(x_1, \dots, x_n) = 1$ and $|\mathbf{x}| \geq H$ lies in $\mathcal{L}_1 \cup \dots \cup \mathcal{L}_t$.

Proof. This is the Corollary of [3]. □

Lemma 11. *Suppose that $F(\mathbf{X})$ is a reduced norm form as in Theorem 2 which satisfies (5). The large solutions of $F(\mathbf{X}) = 1$ lie in at most $2^{1570} 3^{1007} r^3 \log^2 r$ proper linear subspaces of \mathbb{Q}^3 .*

Proof. This is a simple consequence of Lemmas 9 and 10, taking $n = 3, \delta = 1/(2 \cdot 6^{48}), L_1 = M_{i_1}, L_2 = M_{i_2}$ and $L_3 = M_{i_3}$. Since these L_i 's are normalised linear forms coming from our original $L^{(i)}$'s, we have $D \leq 8r^3$ and $H = \max_i H(L^{(i)})$, by the product formula. The lemma then follows from a simple calculation upon noting that $r \geq 4$, that there are $\binom{r}{3}$ possibilities for $1 \leq i_1 < i_2 < i_3 \leq r$ and that $r(r-1)(r-2) \log(32r^3) \log \log(32r^3) < 4r^3 \log^2 r$ for $r \geq 4$. □

Lemma 12. *Let $f(X, Y) = aX^2 + bXY + cY^2$ be a norm form with integer coefficients then the equations $f(X, Y) = \pm 1$ each have at most one family of solutions.*

Proof. This follows from Theorem 5 of Section 2.7 of [1] and the discussion that follows. Theorem 5 states that there is a one-to-one correspondence between the families of solutions of $f(x, y) = m$ and the modules, \mathcal{A} , in a certain class which have norm m and lie in the coefficient ring of the module corresponding to $f(x, y)$ (using their definition of classes of modules and of the norm of a module). The discussion on p. 144 demonstrates that finding such modules reduces to the problem of finding all integers A and B such that $-A \leq B < A$, $B^2 - 4AC$ is the discriminant of f and $m = AS^2$ for some $C, S \in \mathbb{Z}$.

Borevich and Shafarevich show, at the bottom of p. 142 and the top of p. 143 of [1] that it suffices to consider only positive integers m . So, putting $m = 1$, the last condition on A and B shows that $A = 1$. Combining this with the first condition, we find that either $B = 0$ or $B = -1$. This means that $D = -4C$ or $D = 1 - 4C$.

Clearly only one of these can be true and hence there is at most one such module, i.e., at most one family of solutions. \square

5. PROOF OF THEOREM 2

Combining Lemmas 8 and 11, along with our discussion of the relation between solutions of the $F_j(\mathbf{X}) = 1$ and $F(\mathbf{X}) = 1$, we see that the solutions of (3) lie in the union of at most

$$(125\,000^3 + 22) (2^{95} 3^{108} r^9 + 2^{1570} 3^{1007} r^3 \log^2 r) < 1.1 \cdot 10^{965} r^9$$

proper linear subspaces of \mathbb{Q}^3 , since $r \geq 4$.

The integer points in any proper linear subspace of \mathbb{Q}^3 can be parametrised as $\mathbf{x} = T\mathbf{y}$ where T is a linear map from \mathbb{Q}^2 into the subspace which sets up a 1-1 correspondence between \mathbb{Z}^2 and the integer points in the subspace.

Thus, restricting our attention to the integer points of the subspaces which arise, our norm form $F(\mathbf{X})$ becomes $F(T(\mathbf{Y}))$, which is a norm form in two variables with integer coefficients. We may also write them as

$$F_1(\mathbf{Y}) = \mathcal{N}_{\mathbb{K}/bQ} (\beta_1 Y_1 + \beta_2 Y_2) = 1.$$

We must now consider the fields $K_1 = \mathbb{Q}(\beta_1/\beta_2)$. If $[\mathbb{K}_1 : \mathbb{Q}] \geq 3$, then the \mathbb{Z} -module generated by β_1 and β_2 is not a full module and so $F_1(\mathbf{Y})$ is a binary form of degree r which is not a power of a binary quadratic form. Thus, as a consequence of Theorem 1 of [14] (take ϵ sufficiently large), $F_1(\mathbf{Y}) = \pm 1$ has at most $5600r$ integer solutions. We need to consider $F_1(\mathbf{Y}) = \pm 1$, since $F_1(\mathbf{Y})$ might be the power of a binary form of lower degree. So it remains to consider the case when \mathbb{K}_1 is a quadratic field. But by Lemma 12, there are at most two families in this case.

Thus for each subspace there are at most $5600r$ families of solutions. Therefore, by our estimate above for the number of proper linear subspaces of \mathbb{Q}^3 into which the solutions must fall, there are at most $1.1 \cdot 10^{965} \cdot 5600r^{10} < 10^{969} r^{10}$ families of solutions to (3).

6. ACKNOWLEDGEMENTS

This work originated during the author's stays at the University of Colorado in Boulder during the 1990's, first as a graduate student and again as a visiting professor. The author is extremely grateful to Wolfgang Schmidt for his kindness, generosity and support during these periods, financially as well as with his time and ideas.

The author also thanks the referees for their careful reading of this paper and their helpful suggestions. Their advice improved both the results as well as the presentation here and is appreciated.

REFERENCES

- [1] Z.I. Borevich and I.R. Shafarevich, *Number Theory* (Academic Press, New York, 1966).
- [2] E. Bombieri and W. M. Schmidt, On Thue's equation, *Invent. Math.* **88** (1987) 69–81.
- [3] J.-H. Evertse, An improvement of the quantitative subspace theorem, *Compositio Math.* **101** (1996) 225–311.
- [4] J.-H. Evertse, private communication, Sept. 1996.
- [5] J.-H. Evertse and K. Győry, The numbers of families of solutions of decomposable form equations, *Acta Arith.* **80** (1997) 367–394.
- [6] K. Győry, On the numbers of families of solutions of systems of decomposable form equations, *Publ. Math. Debrecen* **42** (1993), 65–101.
- [7] D. A. Marcus, *Number Fields* (Springer-Verlag, New York, 1977).
- [8] P. Ribenboim, *Algebraic Numbers* (Wiley-Interscience, New York, 1972).
- [9] W. M. Schmidt, Linearformen mit algebraischen Koeffizienten. II, *Math. Ann.* **191** (1971) 1–20.
- [10] W. M. Schmidt, Norm form equations, *Ann. of Math.* **96** (1972) 526–551.
- [11] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics 785 (Springer, New York, 1980).
- [12] W. M. Schmidt, The subspace theorem in Diophantine approximations, *Compositio Math.* **69** (1989) 121–173.
- [13] W. M. Schmidt, The number of solutions of norm form equations, *Trans. Amer. Math. Soc.* **317** (1990) 197–227.
- [14] C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.* **4** (1991) 793–835.
- [15] P. M. Voutier, *Effective and quantitative results on integral solutions of certain classes of diophantine equations*, Ph.D. Thesis, Department of Mathematics, University of Colorado, Boulder, 1993.

LONDON, UK, PAUL.VOUTIER@GMAIL.COM